

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF TEXAS**

ALISA SMITH, on behalf of herself and all  
others similarly situated,

*Plaintiffs,*

v.

AT&T, INC.

*Defendants.*

§  
§  
§  
§  
§  
§  
§  
§  
§  
§

CIVIL ACTION NO. \_\_\_\_\_

**CLASS ACTION COMPLAINT**

Plaintiff Alisa Smith (“Plaintiff”), by and through her attorneys, complain and allege as follows:

**INTRODUCTION**

1. This action arises out of AT&T’s failure to secure its customers’ sensitive personal information. In April 2024, AT&T discovered a third party or third parties accessed and captured the private information of approximately 110 million AT&T customers. AT&T’s failure to take reasonable steps to secure its customers’ data, including personally identifiable information (“PII”), will result in identity theft, out-of-pocket loss, and the understandable distress that a person’s private information is now in the hands of criminal hackers. AT&T waited until July 12, 2024 to publicly disclose the data breach and to begin notifying its affected customers.

2. Defendant AT&T is a multinational telecommunications company that provides a wide range of services including landline telephone, mobile telephone, broadband internet, and television services. AT&T promises its customers in a Privacy Notice that it will “work hard to safeguard your information using technology controls and organizational controls,” that AT&T

“protect[s] our computer storage and network equipment,” and that AT&T “limit[s] access to personal information to the people who need access for their jobs.”<sup>1</sup>

3. AT&T now acknowledges that 110 million current and former customers were impacted, and that the exposed information includes call log information. Because the information identifies each telephone number that an AT&T cellular number interacted with during the time period, it also includes the records of consumers who receive their phone service from carriers other than AT&T.

4. AT&T has since provided notices to its customers, acknowledging that based on its investigation to date, the call log information contains the records of calls and text messages, from the six months between May 1, 2022 and October 31, 2022, as well as on January 2, 2023.

5. As a result of AT&T’s failure to honor its contractual commitment to consumers, Plaintiffs and the Class face a heightened, imminent risk of harm in the future. Plaintiff and the Class must now incur the expense and inconvenience of monitoring their financial accounts and credit histories to guard against the increased risk of identity theft, and will incur out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures in order to detect, protect, and repair the data breach’s impact on their lives.

6. This is a class action brought on behalf of a nationwide Class of persons whose information was accessed as a result of AT&T’s failure to adequately protect individuals’ PII and failure to effectively monitor its platform for security vulnerabilities. Plaintiff bring causes of action for breach of contract and negligence. Plaintiffs also bring this action on behalf of a subclass of consumers residing in California for violation of California’s Customer Records Act, Cal. Civil Code §§ 1798.80, et seq., and violation of California’s Unfair Competition Law, Cal. Bus. & Prof.

---

<sup>1</sup> <https://about.att.com/privacy/privacy-notice.html#data-retention> (last visited August 14, 2024).

Code §§ 17200, et seq.

7. Plaintiff seek damages stemming from at least the following:
  - a. Loss of value of personal information;
  - b. Out-of-pocket expenses;
  - c. Benefit of the bargain loss; and
  - d. Punitive damages.

### **PARTIES**

8. Plaintiff Alisa Smith resides, and at all relevant times, resided in Los Angeles, California. She has been an AT&T customer since 2006. On July 15, 2024, she was notified by AT&T over e-mail that her personal information was compromised in the AT&T data breach.

9. Defendant AT&T, Inc. is headquartered at 208 South Akard Street, Dallas, Texas 75202, and may be served via their registered agent CT Corporation System, 1999 Bryan Street, Ste. 900, Dallas, Texas 75201.

### **JURISDICTION AND VENUE**

10. This Court has subject matter jurisdiction over this action under 28 U.S.C. §§ 1332(d) because this is a class action wherein the amount in controversy exceeds \$5,000,000, there are more than 100 members in the proposed Class, and at least one member of the Class is a citizen of a state different from defendant AT&T.

11. This Court has personal jurisdiction over AT&T because AT&T is headquartered in Texas and has purposefully availed itself of the rights and benefits of Texas, including providing services throughout the United States, including in this District; conducting substantial business in this District; and having a registered agent to accept service of process in this District.

12. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events giving rise to the claim occurred in, were directed to, or emanated

from this District. Venue is also proper pursuant to 28 U.S.C. § 1391(b)(1) and (c)(2) because AT&T is subject to the Court's personal jurisdiction in this District.

### **FACTUAL ALLEGATIONS**

#### **A. AT&T's Business**

13. AT&T is one of the largest telecommunications companies in the world, operating in wireless services, wireline services, media and entertainment, business solutions and advertising. AT&T's wireless network reaches more than 210 million people with its nationwide mid-band 5G network to offer, according to it, faster speeds and an enhanced experience on the nation's most reliable 5G network.

14. AT&T collects PII from its customers. It notifies its customers, through an online Privacy Notice available on its website, that "[t]o better run our business, we collect information about you, your equipment and how you use products and services."<sup>2</sup> This information includes contact and billing information, equipment information including phone numbers, location information, web browsing and app information, biometric information such as fingerprints, voice prints, and face scans, and third-party information like credit reports. AT&T acknowledges that "[a]ll these types of information are considered Personal Information when they can reasonably be linked to you as an identifiable person or household."<sup>3</sup>

15. AT&T publicly states in its 2023 Form 10-K that it maintains "a network and information security program that is reasonably designed to protect our information, and that of our customers, from unauthorized risks to their confidentiality, integrity, or availability."

16. In its Privacy Notice, AT&T promises customers that it "work[s] hard to safeguard

---

<sup>2</sup> <https://about.att.com/privacy/privacy-notice.html#collect-information> (last visited August 14, 2024).

<sup>3</sup> *Id.*

your information using technology controls and organizational controls,” “protect[s] our computer storage and network equipment,” “require[s] employees to authenticate themselves to access sensitive data,” and “limit[s] access to personal information to the people who need access for their jobs.”<sup>4</sup>

**B. The Data Breach**

17. AT&T publicly disclosed the data breach at issue (the “Data Breach”) in July 2024.

18. AT&T began notifying customers on or around July 15, 2024 of the Data Breach.

The notice letter said:

We’re reaching out to let you know that some of your data was accessed without authorization. Although we have no current indication of any public release or illegal use of your data, we respect the privacy of your information and want to provide you with details about the event.

The number(s) included in the data attached to your account at the time ended in: [Intentionally Omitted].

**What happened?** We found out AT&T call and text records were accessed by cyber-criminals who have claimed responsibility for unlawful access to other companies in the past. At least one individual has since been arrested.

**What information was involved?** The investigation indicates the data included the phone numbers of your call and text interactions from May 1, 2022 to October 31, 2022. It also included counts of those calls/texts and a total call duration for specific days or months. The data included the cell tower identification number of the most frequently used cell tower over different time periods for some of your call interactions.

**The compromised data does not include the content of calls or text messages nor personal information, such as Social Security numbers, birth dates, or financial information. It also does not include some typical information you see in your usage details, such as the time stamp of calls or texts.**

**What is AT&T doing?** Protecting customer data is a top priority. We have confirmed the affected system has been secured. We hold ourselves to high privacy standards and are always looking for ways to improve our security practices.

**What can you do?** It is always advisable to be careful when taking calls from

---

<sup>4</sup> <https://about.att.com/privacy/privacy-notice.html#data-retention> (last visited August 14, 2024).

numbers that you do not recognize and stay alert to any fraud or theft attempts.

For more information and details about the information that was accessed, go to [att.com/dataincident](https://att.com/dataincident)

For additional tips on privacy and data protection, go to CyberAware.

We apologize for any inconvenience and remain committed to protecting the information in our care.

19. The Call Log Information comprises an array of highly personal information including the phone number of the AT&T customer, the phone numbers that the AT&T customer called or texted, the number of times the AT&T customer interacted with each phone number, and call durations. Many records also included information about the AT&T customers' locations in the form of cell site ID numbers.

20. The collection of personally identifiable information of consumers that has now been stolen, even without the content of calls and texts, enables third parties to identify individual persons and uncover otherwise private and sensitive information about them. As AT&T admits in its press release about the data breach, "there are often ways, using publicly available online tools, to find the name associated with a specific telephone number."

21. Call Log Information can be used to create an intimate portrait of people's lives and relationships. Per Privacy International: "This data is some of the most detailed data that a telephone company holds on its customers . . . Drawing out who is speaking to who, and when gives you a detailed map of our personal lives. This is why law enforcement and intelligence agencies are always trying to get their hands on exactly this data, and it's why it must be secured."<sup>5</sup>

22. Knowledge of a person's physical location, contact habits, and telephone number enables a wide range of fraud, such as impersonating a person's bank or doctor's office to obtain

---

<sup>5</sup> <https://www.bloomberg.com/news/articles/2024-07-12/at-t-hack-undermines-us-national-security-experts-say>

additional sensitive information to do further harm.

23. AT&T has not disclosed any information about the vulnerability that led to the breach. Upon information and belief, AT&T had uploaded the Call Log Information to the servers of a third party called Snowflake, a company that provides cloud-storage services, effectively outsourcing its responsibility to guard the consumer information that was ultimately stolen by hackers. Initial reports indicate that AT&T's account on Snowflake is the result of failing to use multi-factor authentication, which Snowflake made available to its corporate customers, including AT&T. Consequently, AT&T's account on Snowflake could be accessed simply through a username and password.

24. AT&T released a statement following the data breach that described the incident this way:<sup>6</sup>

In April, AT&T learned that customer data was illegally downloaded from our workspace on a third-party cloud platform. We launched an investigation and engaged leading cybersecurity experts to understand the nature and scope of the criminal activity. We have taken steps to close off the illegal access point. We are working with law enforcement in its efforts to arrest those involved in the incident. We understand that at least one person has been apprehended.

Based on our investigation, the compromised data includes files containing AT&T records of calls and texts of nearly all of AT&T's cellular customers, customers of mobile virtual network operators (MVNOs) using AT&T's wireless network, as well as AT&T's landline customers who interacted with those cellular numbers between May 1, 2022 – October 31, 2022. The compromised data also includes records from January 2, 2023, for a very small number of customers. The records identify the telephone numbers an AT&T or MVNO cellular number interacted with during these periods. For a subset of records, one or more cell site identification number(s) associated with the interactions are also included.

The data does not contain the calls or texts, personal information such as Social Security numbers, dates of birth, or other personally identifiable information. It also does not include some typical information you see in your usage details, such as the time stamp of calls or texts. While the data does not include customer names, there are often ways, using publicly available online tools, to find the name

---

<sup>6</sup> <https://about.att.com/story/2024/addressing-illegal-download.html> (last visited August 14, 2024).

associated with a specific telephone number.

At this time, we do not believe that the data is publicly available.

Our top priority is, as always, is our customers. We will provide notice to current and former customers whose information was involved along with resources to help protect their information. We sincerely regret this incident occurred and remain committed to protecting the information in our care. Customers can visit [att.com/DataIncident](https://att.com/DataIncident) for more information.

### **C. Consequences of the AT&T Data Breach**

25. The potential consequences of the Data Breach are substantial. Plaintiff and Class members face a heightened risk that identity thieves will open financial accounts in their names, open credit cards in their names, use their information to obtain government benefits, file fraudulent tax returns to obtain tax refunds, obtain driver's licenses or identification cards in their names, gain employment in their names, obtain medical services in their names, or give false information to police during an arrest. Hackers also commonly sell personal information to other criminals to enable them to misuse the information.

26. Private information is valuable property. Its value is axiomatic, considering the market value and profitability of "Big Data" corporations in America. Illustratively, Alphabet Inc., the parent company of Google, reported in its 2020 Annual Report a total annual revenue of \$182.5 billion and net income of \$40.2 billion. \$160.7 billion of this revenue derived from Alphabet's Google business, which is driven almost exclusively by leveraging the private information it collects about the users of its various free products and services.

27. Criminal law also recognizes the value of PII and the serious nature of its theft by imposing prison sentences on cyber thieves, who can earn significant revenue through stealing PII. Once a cybercriminal has unlawfully acquired personal data, the criminal can demand a ransom or blackmail payment for its destruction, use the information to commit fraud or identity theft, or sell the PII to another cybercriminal on a thriving black market. Cybercriminals use "ransomware" to

make money and harm victims. Ransomware is a widely known and foreseeable malware threat in which a cybercriminal encrypts a victim's computer such that the computer's owner can no longer access any files or use the computer in any way. The cybercriminal then demands a payment for the decryption key. Ransomware is typically propagated through phishing, spear phishing, or visiting a malicious or compromised website that contains a virus or other malware.

28. Once stolen, PII can be used in a number of different ways. One of the most common is to offer it for sale on the "dark web," a heavily encrypted part of the Internet that makes it difficult for authorities to detect the location or owners of a website. The dark web is not indexed by normal search engines such as Google and is only accessible using a Tor browser (or similar tool), which aims to conceal users' identities and online activity. The dark web is notorious for hosting marketplaces selling illegal items such as weapons, drugs, and PII. Websites appear and disappear quickly on the dark web, making it a dynamic environment.

29. Recently, the Organization for Economic Cooperation and Development estimated the prices for various elements of personal data: \$0.50 for an address, \$2 for birthdate, \$8 for a Social Security number, \$3 for a driver's license number, and \$35 for a military record. The value of personal data continues to be high: a personal email can be worth \$89, a complete health care record \$250, and a hacked Facebook account can sell for \$65 on the dark web. Similarly, a 2019 report found that data generated from an adult is worth roughly \$35 per month.

30. The FTC recommends that identity theft victims take several steps to protect their personal information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and to consider an extended fraud alert that lasts for seven years if identity theft occurs), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.

31. Cybercriminals use stolen PII such as social security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. Identity thieves can also use social security numbers to obtain a driver's license or other official identification card in the victim's name, but with the thief's picture; use the victim's name and social security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's social security number, rent a house or receive medical services in the victim's name, seek unemployment or other benefits, and may even give the victim's PII to police during an arrest resulting in an arrest warrant being issued in the victim's name. Obtaining a new social security number is difficult and rarely occurs.

32. Furthermore, data breaches that expose any personal data directly and materially increase the chance that a potential victim is targeted by a spear phishing attack in the future. Spear phishing results in a high rate of identity theft, fraud, and extortion.

33. Unfortunately for Plaintiff and Class members, a person whose personal information has been compromised may not fully experience the effects of the data breach for years to come:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.<sup>7</sup>

34. As a result of the Data Breach, Plaintiff and Class members have and will continue to incur out-of-pocket costs and expenses for, among other things, purchasing credit monitoring

---

<sup>7</sup> <https://www.gao.gov/new.items/d07737.pdf> (last visited August 14, 2024).

services, credit freezes, credit reports, and/or other protective measures to deter and detect identity theft. Plaintiff and Class members have and will continue to spend time, resources, and money to mitigate their damages from the Data Breach, and they remain at a heightened and imminent risk of fraud and identity theft. Plaintiff and Class members must now and in the future closely monitor their bank accounts and credit card accounts to guard against the risk of identity theft.

35. Protections that are necessary to users whose security was hacked include identity theft and credit monitoring, which tends to cost roughly \$18 to \$30 per month, and identity theft insurance, which ranges from \$25 to \$60 per year, if not more.

36. In sum, the costs to date of AT&T's negligent handling of consumers' information are significant, ranging from intangible loss of privacy to tangible financial harm, both known and unknown. Meanwhile, a user taking reasonable precautions to obtain identity theft and credit monitoring and identity theft insurance would have to spend between \$241 and \$420 per year.

37. At all relevant times, AT&T knew, or reasonably should have known, of the importance of safeguarding customers' personal information and the reasonably foreseeable consequences that would occur if its data systems were breached, including, specifically, the significant costs that would be imposed on consumers as a result of a breach. Indeed, AT&T should have been particularly aware of its obligations and the potential consequences of not fulfilling its obligations as it very recently experienced a massive data breach that it disclosed in March 2024 involving the PII of 73 million of AT&T's current and former customers that was discovered on the "Dark Web."

38. The Data Breach was a direct and proximate result of AT&T's failure to properly safeguard and protect Plaintiff's and Class members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common

law, including AT&T's failure to establish and implement appropriate technical safeguards to ensure the security and confidentiality of Plaintiff's and the Class members' PII to protect against reasonably foreseeable threats to its security or integrity.

39. AT&T's wrongful actions and inaction directly and proximately caused the theft and dissemination to an unknown third party of Plaintiff's and Class members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

- a. theft of their PII;
- b. costs for credit monitoring services;
- c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and already misused via the sale of Plaintiff's and Class members' PII on the dark web;
- d. the improper disclosure of their data;
- e. loss of privacy;
- f. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;
- g. ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market;
- h. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, changing the information used to verify their identity to

information not subject to this Data Breach, and the stress, nuisance and annoyance of contending with all such issues resulting from the Data Breach.

**CLASS ACTION ALLEGATIONS**

40. Plaintiff brings this action on behalf of herself and as a class action under Fed. R. Civ. P. 23(b)(2) and (b)(3) on behalf of:

All natural persons residing in the United States whose personal information was accessed as a result of the AT&T data breach announced in July 2024 (the “Class”).

41. Plaintiff also brings this action on behalf of:

All natural persons residing in California whose personal information was accessed as a result of the AT&T data breach announced in July 2024 (the “California Subclass”).

42. The members of the Class are so numerous that joinder of all members is impracticable. While the exact number of class members is unknown to Plaintiff at this time and can only be ascertained through appropriate discovery, Plaintiff believes there are 110 million members of the Class. The identities of absent members of the Class are ascertainable because they may be identified from records maintained by AT&T and may be notified of the pendency of this action by mail, using a form notice similar to that customarily used in consumer class actions.

43. There are questions of law and fact common to the Class, including:

a. Whether AT&T’s response to the Data Breach fell below commercially reasonable standards with respect to the protection of that information;

b. Whether AT&T implemented and maintained reasonable security procedures and practices appropriate to storing Plaintiff’s and Class members’ personal information;

c. Whether AT&T acted negligently in connection with its monitoring and protection of Plaintiff and Class members’ personal information;

d. Whether the data breach was made possible by AT&T's substandard data security measures and practices;

e. Whether AT&T adequately addressed and fixed the vulnerability that permitted the Data Breach to occur;

f. Whether Plaintiff and other Class members are entitled to credit monitoring and other monetary relief;

g. Whether AT&T violated California consumer privacy and unfair competition laws; and

h. The appropriate Class-wide measure of damages.

44. At the time of the Data Breach, Plaintiff and Class members had their personal information stored on AT&T's servers. Plaintiff's claims are typical of the claims of the Class, and Plaintiff will fairly and adequately protect the interests of that Class.

45. The questions of law and fact common to the members of the Class predominate over any questions affecting only individual members, including legal and factual issues relating to liability and damages.

46. Plaintiff is represented by counsel who are competent and experienced in the prosecution of class action litigation.

47. The prosecution of separate actions by individual members of the Class would also create a risk of inconsistent or varying adjudications, establishing incompatible standards of conduct for AT&T.

48. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Individual claims are likely too small to prosecute economically on an individual basis. Prosecution as a class action will eliminate the possibility of repetitious

litigation. Treatment as a class action will permit a large number of similarly situated persons to adjudicate their common claims in a single forum simultaneously, efficiently, and without the duplication of effort and expense that numerous individual actions would engender. This class action presents no difficulties in management that would preclude maintenance as a class action.

### **CLAIMS FOR RELIEF**

#### **FIRST CLAIM FOR RELIEF**

##### **Breach of Contract**

##### **(On Behalf of the Nationwide Class)**

49. Plaintiff, on behalf of herself and the Class, incorporate and re-allege the preceding paragraphs of the complaint.

50. AT&T's Privacy Notice is an agreement between AT&T and its customers who provided their PII to AT&T, including Plaintiff and Class members.

51. AT&T's Privacy Notice states, among other things, that it applies to "AT&T products and services including internet, wireless, voice and AT&T apps" and the Privacy Notice "explains how we use your information and keep it safe."<sup>8</sup> According to AT&T, it collects "personal information" that "can reasonably be linked to you as an identifiable person or household." The Privacy Notice states that AT&T "work[s] hard to safeguard your information using technology controls and organizational controls," that AT&T "protect[s] our computer storage and network equipment," and AT&T "limit[s] access to personal information to the people who need access for their jobs."<sup>9</sup> AT&T further promised that it would only share certain data under specific enumerated circumstances, which includes "with your consent" or with AT&T companies and its affiliates for specified purposes such as identity verification, providing a service,

---

<sup>8</sup> <https://about.att.com/privacy/privacy-notice.html> (last visited August 14, 2024).

<sup>9</sup> *Id.*

and for advertising and marketing. None of the enumerated circumstances involve sharing class members' PII with a criminal hacker. In addition, AT&T states that "[i]f a breach occurs, we'll notify you as required by law."

52. AT&T's Privacy Notice also provides for data-retention policies. It states:

We keep your information as long as we need it for business, tax or legal purposes. We set our retention periods based on things like what type of personal information it is, how long it's needed to operate the business or provide our products and services, and whether it's subject to contractual or legal obligations. These obligations might be ongoing litigation, mandatory data retention laws or government orders to preserve data for an investigation. After that, we destroy it by making it unreadable or indecipherable.<sup>10</sup>

53. Plaintiff and Class members provided their PII to AT&T when they, among other things, used AT&T's services and purchased products from AT&T. Consequently, Plaintiff and Class members who transacted with AT&T manifested their willingness to enter into a bargain with AT&T and intention to assent to the terms of the Privacy Notice by providing their PII to AT&T.

54. Conversely, AT&T, in collecting Plaintiff's and Class members' PII, manifested its intent to adhere to its obligations under the Privacy Notice, including "work[ing] hard to safeguard your information using technology controls and organizational controls."

55. Plaintiff and Class members on the one hand and AT&T on the other formed contracts when Plaintiff and Class members provided PII to AT&T subject to its Privacy Notice.

56. Plaintiff and Class members fully performed their obligations under the contracts with AT&T.

57. AT&T breached its agreement with Plaintiff and Class members by failing to protect their PII. Specifically, AT&T (1) failed to take reasonable steps to use safe and secure

---

<sup>10</sup> <https://about.att.com/privacy/privacy-notice.html#data-retention> (last visited August 14, 2024).

systems to protect that information; (2) disclosed that information to unauthorized third parties; and (3) failed to promptly alert or give notice of the breach as required by law.

58. AT&T further breached its agreement with Plaintiff and Class members who are former AT&T customers by failing to comply with its promised data-retention policies. AT&T failed to destroy the data as promised, compromising the sensitive PII of Plaintiff and Class members.

59. As a direct and proximate result AT&T's breaches of contract, Plaintiff and Class members sustained actual losses and damages as described in detail above, and are also entitled to recover nominal damages.

## **SECOND CLAIM FOR RELIEF**

### **Negligence**

#### **(On Behalf of the Nationwide Class)**

60. Plaintiff, on behalf of herself and the Class, incorporate and re-allege the preceding paragraphs of the complaint.

61. AT&T owed a duty to Plaintiff and the Class members to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting and protecting their PII. This duty included designing, maintaining, monitoring and testing AT&T's security systems and protocols to ensure that Class members' PII was protected; implementing processes that would detect a breach of its security system in a timely manner; implementing and utilizing processes to ensure that the transfer of Plaintiff's and Class Member' data between AT&T and third parties was secured and protected; timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and maintaining data security measures consistent with industry standards. AT&T's duty rose independently of any contract.

62. In providing their PII, Plaintiff and Class members had a reasonable expectation that this information would be securely maintained and not easily accessible to, or exfiltrated by cybercriminals.

63. AT&T had a common law duty to prevent foreseeable harm to others. Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices. It was foreseeable that Plaintiff and Class Members would be harmed by the failure to protect their PII because hackers are known to routinely attempt to steal such information and use it for nefarious purposes.

64. AT&T also had a duty to use reasonable security measures required under Section 5 of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45(a), which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect consumers’ PII.

65. AT&T had a special relationship with Plaintiff and Class members because it was entrusted with their personal information, which provided an independent duty of care. AT&T had a duty to use reasonable security measures because it undertook to collect, store, and use consumers’ PII. AT&T was responsible for and in the position to ensure that it implemented sufficient security measures to protect against the foreseeable risk of harm to Plaintiff and Class members from a resulting data breach.

66. AT&T also had a duty to safeguard the PII of Plaintiff and Class members and to promptly notify them of a breach because of state laws and statutes that require AT&T to reasonably safeguard sensitive personal information, as alleged herein.

67. Timely notification of the breach was required so that, among other things, Plaintiff and Class members could take measures to freeze or lock their credit profiles, avoid unauthorized

charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to try to prevent identify theft.

68. Class members whose information was stored by AT&T have an interest in the protection of their PII.

69. AT&T breached its duty to exercise reasonable care in protecting Plaintiff's and Class members' PII by:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class members' PII, including failing to use Multi-Factor Authentication;
- b. Failing to adequately monitor the security of its networks and systems;
- c. Failing to implement and utilize processes to ensure that the storage of Plaintiff's and Class Members' PII on third-party platforms was secured and protected;
- d. Allowing unauthorized access to and exfiltration of Plaintiff's and Class members' PII; and
- e. Failing to provide timely notice by delaying for several months since the breach began, that Plaintiff's and Class members' PII had been compromised so those at risk could take timely and appropriate steps to mitigate the potential for identity theft and other damages.

70. Plaintiff's and Class members were the foreseeable victims of AT&T's inadequate and ineffectual cybersecurity. The natural and probable consequence of AT&T failing to implement adequate security was Plaintiff's and Class members' PII being hacked.

71. AT&T knew or should have known that Plaintiff's and Class members' PII was an attractive target for cyber thieves, particularly in light of data breaches experienced by other entities around the United States. Moreover, the harm to Plaintiff and Class members from exposure of their highly confidential personal facts was reasonably foreseeable to AT&T.

72. It was foreseeable to AT&T that their failure to use reasonable measures to protect Plaintiff's and Class members' PII, including when it warned its systems and networks were vulnerable to cyberattack, would result in injury to Plaintiff and Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of ransomware attacks and data breaches.

73. It was also foreseeable to AT&T that its failure to timely notify customers of the breach would result in Plaintiff and Class members not being afforded the ability to timely safeguard their identities.

74. There is a close connection between AT&T's failure to employ reasonable security protections for the PII and the injuries suffered by Plaintiff and Class members. When individuals' sensitive personal information is stolen, they face a heightened risk of identity theft and may need to: (1) purchase identity protection, monitoring, and recovery services; (2) flag asset, credit, and tax accounts for fraud, including by reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the IRS; (3) purchase or otherwise obtain credit reports; (4) monitor credit, financial, utility, explanation of benefits, and other account statements on a monthly basis for unrecognized credit inquiries and charges; (5) place and renew credit fraud alerts on a quarterly basis; (6) contest fraudulent charges and other forms of identity theft; (7) repair damage to credit and financial accounts; and (8) take other steps to protect themselves and attempt to avoid or recover from identity theft and fraud.

75. The policy of preventing future harm disfavors application of the economic loss rule, particularly given the sensitivity of the PII entrusted to AT&T. AT&T had an independent duty in tort to protect this information and thereby avoid reasonably foreseeable harm to Plaintiff and Class members.

76. AT&T's negligence was gross, willful, wanton, and reprehensible and warrants the imposition of punitive damages given the clear foreseeability of a hacking incident, the extreme sensitivity of the private information under AT&T's care, and its failure to timely notify the victims.

77. Plaintiff and the Class have suffered injury in fact and a loss of money or property in the following ways:

- a. They have had their present and future property interest in their personally information diminished;
- b. They have been deprived of control over their personal information;
- c. They may be required to incur the expense of credit report freezes, credit and identity theft monitoring, and identity theft insurance; and
- d. They are at imminent risk of future harm from identity theft.

78. The damages to Plaintiff and Class members were a proximate, reasonably foreseeable result of AT&T's breach of its duties to safeguard the consumers' PII it was entrusted to keep.

79. Plaintiff and Class members are entitled to damages in an amount to be proven at trial.

**THIRD CLAIM FOR RELIEF**

**Violation of California's Unfair Competition Law ("UCL"),**

**Cal. Bus. & Prof. Code §§ 17200, *et seq.***

**(On Behalf of the California Subclass)**

80. Plaintiff, on behalf of herself and the California Subclass, incorporate and re-allege the preceding paragraphs of the complaint.

81. AT&T has engaged in unlawful, unfair and deceptive practices, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect plaintiff and California Subclass members' personal information, which was a direct and proximate cause of the AT&T data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures, which was a direct and proximate cause of the AT&T data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the AT&T data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and California Subclass members' personal information, including by implementing and maintaining reasonable data security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California

Subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and California Subclass members' personal information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' personal information, including duties imposed by the FTC Act.

82. Plaintiffs and the California Subclass members have suffered injury in fact and a loss of money or property in the following ways:

a. They have had their present and future property interest in their PII diminished;

b. They have been deprived of the exclusive use of their PII;

c. They may be required to incur expenses in connection with obtaining credit report freezes, credit and identity theft monitoring, and identity theft insurance; and

d. They are at imminent risk of future harm from identity theft.

83. AT&T's actions were unlawful in that they violated the FTC Act, 15 U.S.C. § 45(n) (allowing the FTC to declare unlawful an act or practice that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition").

84. AT&T's actions were also fraudulent in that they represented a standard of care that it knew or should have known to be false.

85. Had AT&T disclosed to Plaintiff and California Subclass members that its data systems were not secure and, thus, vulnerable to attack, AT&T would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, AT&T was trusted with sensitive and valuable personal information of millions of consumers, including Plaintiff and California Subclass members. AT&T accepted the responsibility of maintaining consumer data while keeping the inadequate state of its security controls secret from the public.

86. AT&T had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity of the personal information in its possession, and the generally accepted professional standards in the telecommunications industry. Such a duty is also implied by law due to the nature of the relationship between consumers—including Plaintiff and the California Subclass—and AT&T, because consumers are unable to fully protect their interests with regard to the personal information in AT&T's possession, and place trust and confidence in AT&T. AT&T's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of consumers' data stored in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, while purposefully withholding material facts from Plaintiff and Class members that contradicted these representations.

87. As a direct and proximate result of AT&T's unfair and deceptive acts or practices, Plaintiff and California Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including

from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their personal information.

88. Plaintiff and California Subclass members are entitled to restitution in the form of the diminished value of the personal information that was entrusted to AT&T.

**PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiff prays as follows:

- A. Certifying this case as a class action, appointing Plaintiff as Class representative, and appointing interim class counsel to represent the Class;
- B. Entering judgment for Plaintiff and the Class;
- C. Awarding Plaintiff and Class members actual damages, compensatory damages, punitive damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;
- D. Ordering appropriate injunctive relief, including improving AT&T's cybersecurity practices;
- E. Awarding pre- and post-judgment interest according to law;
- F. Awarding reasonable attorneys' fees and costs as permitted by law;
- G. Granting such further and other relief as may be just and proper.

Dated: August 15, 2024

Respectfully submitted,

SUSMAN GODFREY L.L.P.

/s/ Barry Barnett

Barry Barnett  
TX State Bar No. 01778700  
1000 Louisiana Street, Suite 5100  
Houston, Texas 77002-5096  
Telephone: (713) 651-9366

Fax: (713) 654-6666  
bbarnett@susmangodfrey.com

Krysta K. Pachman (*pro hac vice forthcoming*)  
Michael Gervais (*pro hac vice forthcoming*)  
1900 Avenue of the Stars, Suite 1400  
Los Angeles, California 90067  
Telephone: (310) 789-3100  
Fax: (310) 789-3150  
kpachman@susmangodfrey.com  
mgervais@susmangodfrey.com

*Attorneys for Alisa Smith, on behalf of herself  
and all others similarly situated*

**DEMAND FOR JURY TRIAL**

Plaintiff requests a jury trial on all matters so triable.

DATED: August 15, 2024

BARRY BARNETT  
KRYSTA KAUBLE PACHMAN  
MICHAEL GERVAIS

SUSMAN GODFREY L.L.P.

/s/ Barry Barnett

Barry Barnett  
Attorney for Plaintiff